金融行业开源技术应用社区
FINANCE OPEN SOURCE

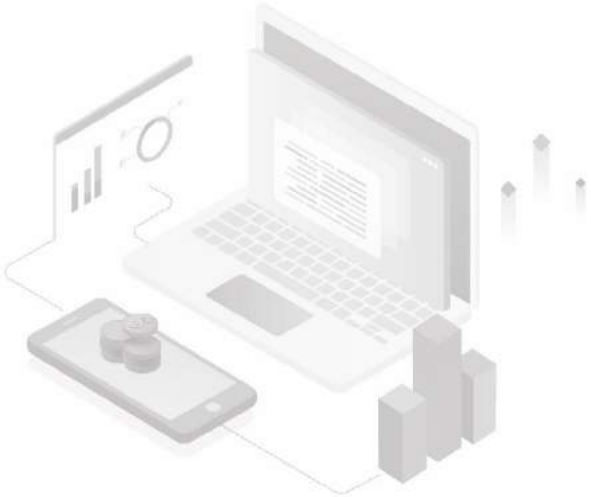
云计算开源产业联盟
OpenSource Cloud Alliance for IndustRy,OSCAR

金融行业开源治理白皮书

（2019年）

金融行业开源技术应用社区　云计算开源产业联盟

2019年7月



版权声明

编写说明

编写单位：中国信息通信研究院、上海浦东发展银行股份有限公司、中国农业银行股份有限公司、中信银行股份有限公司、中国太平洋保险(集团)股份有限公司、上海银行股份有限公司、中国人寿保险股份有限公司、上海农村商业银行股份有限公司、

编写人： 栗蔚、郭雪、武倩聿、万化、杨欣捷、彭颖、叶馥郁、赖强、李玉省、陈建锋、邓琼、张文若、郑位威、裴玉平、苏福江、倪焰

目 录

前　言

近几年开源技术快速发展，金融行业在构建信息系统过程中不可避免涉及开源技术的引入和使用。开源一方面可以突破技术壁垒推动金融机构技术创新和业务发展，另一方面也不可避免的带来知识产权、信息安全等一系列问题。金融作为涉及关乎国民经济的关键行业，面临与其他行业相比更为严苛的监管要求。如何在遵循开源义务要求的前提下规范地使用开源技术，从而最大化减少使用开源带来的风险，是金融机构构建信息系统过程中必然面临的问题。

《金融行业开源治理白皮书》首先介绍企业用户引入开源技术的背景，阐述开源技术对金融行业的重要意义，重点梳理引入开源可能导致的风险，并对金融行业在开源治理方面可以采取的措施给出了建议，最后附录了参与白皮书撰写企业的开源治理实践案例。

金融行业开源治理白皮书

一、 开源技术迅猛发展推动企业引入开源

近几年开源技术快速发展，在云计算、移动互联网、大数据等领域逐渐形成技术主流。开源技术正在渗透软件领域的方方面面，企业用户已经越来越难以规避开源的引入。与此同时，开源的迅猛发展也推动企业从购买闭源商业软件转向关注和使用开源软件。整体而言，不论企业是否接受，开源已经从事实上成为了一种不可阻挡的趋势。

1、开源已在多个重要领域成为主流

开源推动软件生产模式向多人协作方向发展。相比于闭源软件封闭式的开发模式，开源软件开放式的生产模式推动更多人参与到软件的创造之中。最初，大多数自由和开源软件项目的贡献者通过电子邮件或私有的版本控制系统（如 Subversion 或 BitKeeper）进行协作。诞生于 2008 年的 GitHub 改变了这一情况，GitHub 提供使用 Git 进行版本控制的软件源代码托管服务，使更多开发者能够更方便地参与开源项目，进一步推动开源软件生产效率和生产质量的提升。GitHub 的出现改变了开源软件的协作模式，开发者不再需要先获得开发者社区的权限才能参与开源项目，这种多人协作的软件生产模式大大推动了开源软件市场的发展壮大。

开源软件已经逐步形成强大的生态链条。21 世纪之前，软件世界以闭源为主，“闭源”与“收费”成为软件市场的主流，IBM、甲骨文、EMC 为核心的软硬件产品是金融行业用户的主要选择。90 年代末，开源软件从对商业软件的模仿开始兴起，如：Linux（对应微软的 Windows 操作系统）、OpenOffice（对应微软的 Office）、FuseESB（对应 IBM ESB 和 Oracle ESB）等等。从 00 年代到现在，开源软件在市场上已经逐步与闭源软件平分秋色。近年来，随着 IT 产业逐渐向服务化转型，开源已经成为 ICT 产业发展的重要趋势，在移动互联网、云计算、大数据、人工智能等诸多重要领域成为主流技术形态，如：移动互联网领域的 Android，云计算领域的 OpenStack、Kubernetes(k8s)，大数据领域的 Hadoop，人工智能领域的 Tensorflow 等。以上领域的技术更新迭代速度较快，企业用户在选择相关领域技术时，可能存在没有商业产品可供选择，只能被迫采用开源技术的现象。

2、企业用户引入开源技术不可避免

随着开源技术快速形成生态，企业用户引入开源技术已成大势所趋。一方面，开源技术已经在大数据、云计算等重要领域形成技术主流，开源软件覆盖软件生态的诸多方面；另一方面开源代码规模正在飞速增长，截至 2018 年 9 月，开源代码托管平台 GitHub 上已经有 9600 多万个库，相比去年也增长了 40% 以上。

由此可见，开源软件已经成为软件生态的重要且不可替代的组成部分，不论管理者是否知悉，企业内部在很大概率上都已经引入了开源相关的技术，具体有以下三种引入形式：

1）所购买或使用的商业软件，隐含开源组件或代码

在开源软件兴起之前，大多数企业一般会选择购买商业软件，因为这种购买行为对于企业而言是“公对公”的，大企业内部一般都有规范的采购流程，企业负责人也认为商业软件的售后有所保障。

然而，并不是购买了商业软件就意味着不用关心开源。实际上，很多商业软件是基于开源做二次开发后以闭源形式提供给用户的，但用户一般只知道自己购买了商业软件，而对其中可能涉及的开源风险一无所知。

如果用户没有特殊要求，商业软件供应商一般不会说明是否涉及开源软件，而用户一般不能直接接触到软件的源代码。因此，用户很可能被动的就引入了开源软件，即使想遵守开源规则也无从下手。虽然企业用户确实购买了商业软件，但商业软件中却有可能包含开源的成分，用户很可能在不知情的情况下使用了开源而不自知。从这个角度来说，很多时候并不是企业用户主动选择了开源，而是被动使用了开源之后才意识到了解开源的重要性。

2）购买基于开源软件的商业版本

很多时候企业觉得自己购买了商业软件，然而实际上却往往是开源的商业版或者是发行版。目前已知的 Linux 发行版就有

300 多种，其中就有比较成功的商业发行版如：redhat、SUSe、Ubuntu 等；全球范围内基于 OpenStack 提供支持和服务的企业超过 150 家，根据 OpenStack 基金会发起的第 11 次全球 OpenStack 用户调查显示，华为、红帽、 EasyStack（易捷行云）是 2018 年排名前三甲的 OpenStack 软件供应商；大数据领域的 Hadoop 除了 Apache 的版本之外，华为发行版、Intel 发行版、Cloudera 发行版和 DKhadoop 发行版均有广泛应用，其中很多发行版都是收费的商业软件。

基于开源的商业版通常有两种情况，一种是双许可证，一种是依商业许可重新发行。

所谓的双许可证是指其软件是基于开源许可证的，但是还有不同的许可条款。用户可以无偿使用无须付费的、开源的版本，这仍然属于商业版本的一部分，若用户有进一步的需求，诸如商业的技术支持和服务则需要另行付费。作为全球领先的数据库软件，MySQL 产品采取了开源许可与私有许可的双重许可模式。MySQL 公司对产品代码拥有完整的著作权(copyright)。在开源许可之下，软件的源代码完全公开，任何人都可以下载 MySQL 软件来使用、修改和传播。如果某商业客户希望在其商业软件中集成 MySQL 并保持原有软件的私有性，那么必须选择私有许可，即向 MySQL 公司支付一定的许可费。采用混合许可的优点在于通过许可协议差异化来最大化产品网络外部性带来的收益。

而依商业许可重新发行则是指一些宽松的许可证，如 Apache、

BSD 等，是允许以商业且闭源的方式二次发行的。这其中最为著名的例子就是苹果公司的 MacOSX 操作系统，其内核是使用的 BSD Unix，但是其二次发行也是顺理成章。这样的方式，也是我们本土常见的方式，比如 OpenStack 采用是非常宽松的 Apache 协议，再次商业发行，包括自己修改的、新增的代码是可以不开源的。

3）直接使用社区版开源软件

目前，开源软件已经覆盖了软件生态的诸多方面，操作系统有 Linux 以开源形式提供，数据库 MySQL、MongoDB 等，云计算领域的 OpenStack 和 Kubernetes(k8s)都是开源技术，新兴领域如区块链技术基本是完全建立在开源的基础上的。

一方面，开源软件更新速度快，相比于商业软件技术迭代速度更快，很多新技术往往都是从开源软件开始，市场广泛认可之后才逐步产生一些商业软件或商业服务。很多时候并不是工程师主动选择了开源，而是因为开源软件的生态相比于商业软件要庞大数倍，使用者只能被动选择开源；

另一方面，开源软件代码公开容易获取，对于企业的工程师而言，大到采用能够独立部署独立运行的软件，小到将 GitHub 上的一段开源代码复制粘贴到自己的代码中，其实都涉及到使用开源的问题。

开源软件已经成为软件生态不可或缺的重要组成部分，很多时候企业经常会直接使用开源软件的社区版，或者直接使用 GitHub 上的组件/代码片段，这些都属于使用了开源。从这个角

度来看，开源已经渗透到了企业信息系统的各个角落，企业对于开源的使用是无处不在且不可逆转的。

二、 金融行业采用开源技术已成趋势

开源软件市场巨大，从基础软件到应用软件都充斥着大量的开源软件。受金融机构转型推动和生态合作伙伴影响，为满足金融用户的实际需求，开源技术已经逐步成为金融机构构建信息系统的重要选择。金融行业采用开源技术已经成为一种趋势，开源技术可以助力金融机构提高科技实力、协助保障信息系统安全、进一步推动企业科技创新和业务创新。

1、开源技术是构建信息系统的重要选择

金融行业相比于新兴的互联网等行业面临更严格的监管要求，因此在引入开源软件方面一直相对慎重。开源技术大规模兴起之前，金融行业往往通过正规采购流程购买商业软件，以满足本企业在信息系统构建方面的需求。

随着时代的变迁和技术的进步，金融机构的 IT 技术方案逐渐从闭源走向开源。金融行业选择开源技术的原因主要有以下三点：

第一，提高敏捷开发效率，满足金融用户需求。随着互联网公司涉足金融领域并开启移动支付时代，目前我国移动支付规模已经稳居全球第一，并逐渐向世界各国拓展。面对金融用户需求

和使用习惯的变化，传统金融机构已经无法完全满足用户需求，互联网金融、数字金融、金融科技等概念纷纷出现，传统金融机构开始创建金融科技公司或成立金融科技部门，金融行业逐步向互联网敏捷开发方向发展。在此过程中，开源技术的引入可以大大提高开发效率和迭代速度，帮助金融机构快速推动业务创新，进一步满足金融用户的需求。

第二，加速海量数据处理，推动金融机构转型。在大规模、高并发、渠道类应用日益增多的互联网金融背景下，金融机构面临向数字化、智能化方向转型的要求。与此同时，机构内海量数据处理、分析需求开始增多，而开源技术可以帮助金融企业构建更敏捷高效、精细化管理、可管可控以及可扩展的 IT 系统，进一步推动金融机构的转型和创新。

第三，主动拥抱开源技术，助力生态伙伴合作。金融机构并不是独立存在的个体，其生态链条上存在各种类型的合作伙伴企业。从供应角度来看，金融机构与科技公司存在密不可分的关系，也不可避免地会受到科技公司在技术方面的影响。鉴于目前开源技术在科技公司当中应用的广泛性，金融机构不可避免会涉及到相关技术，这一变化也将推动传统金融机构逐步从封闭走向开放，进一步促进金融行业转型与发展。

从开源技术的应用与发展角度来看，十年前，操作系统主要是 AIX、HPUnix 等，存储以 EMC、HP 为主，中间件使用 Tuxedo 等，主流的数据库有 Informix、DB2、SQL Server……而目前 Linux

操作系统，Hadoop 分布式文件系统(HDFS)，数据库 MongoDB 和 MySQL，中间件 Kafka、RabbitMQ 等已经在相应领域形成技术主流，很多金融机构也正在使用这些开源技术。

开源技术的发展推动金融机构逐步接受开源和使用开源，开源软件已经渗透到了金融机构软件研发的各个流程。在金融机构中，从管理角度可以将开源软件分为两大类：

第一类是基础类开源软件。指独立部署、独立运行，为应用系统提供基础服务的开源软件，包括操作系统、数据库、中间件等。这类软件一般由独立的专职团队（如运维中心）统一负责管理，包括：编制相关应用部署规范、上线后的运行和维护等。

第二类是应用开发类开源软件。包括开发过程中涉及的开发框架、开发语言、开发工具，以及配置、测试、运维和办公等过程中使用的工具软件等。这类软件一般由引入和使用部门直接管理，负责软件的运行维护工作。

2、选择开源技术对金融机构意义重大

1）开源技术助力金融机构提高科技实力

金融领域的关键信息基础设施是经济社会运行的神经中枢，金融业务高度依赖金融网络和信息系统。《软件和信息技术服务业“十二五”发展规划》中提出要把开源软件作为扶持发展的对象。开源软件具有公开、使用、修改、分发的特点，使用开源软件的机构可以掌握软件的源代码，一方面改善过去采购闭源软件存在

的代码不透明等问题，另一方面也可以弱化商业封闭式系统架构导致的厂商绑定。金融用户通过掌握软件源代码提高对信息系统的把控能力，基于开源代码进行二次开发可以进一步提高金融机构的技术水平和科技实力。

2） 开源技术是金融机构保障信息安全的重要选择

金融作为涉及关乎国民经济的关键行业，面临与其他行业相比更为严苛的监管要求。信息安全已经上升到国家战略层面，信息安全被划入“十三五”重点建设方向、网络安全被正式划入“十三五”规划重点建设方向，在政府未来 5 年的 100 项重大建设项目中排在第六位。

因行业性质原因，金融行业对信息系统安全和软件使用有极高的要求，陆续出台相关行业规范和管理规定，如：《金融行业信息系统信息安全等级保护实施指引》、《中小金融机构灾备云安全要求》、《保险机构信息化监管规定》、《保险公司信息系统安全管理指引（试行）》等。

相比于闭源商业软件，开源软件的源代码更加公开透明。同时，得益于开源生态日趋成熟，PaaS、中间件、数据库等领域开源技术层出不穷，主流的技术基本都有热门的开源软件可供金融机构进行选择。金融机构在进行软件选型时，也可以通过公开的数据对软件进行多方面的评测，通过选择合适的开源技术替代商业软件，助力金融机构有效保障数据安全。

3） 开源技术推动金融机构科技创新和业务创新

为应对互联网金融崛起和竞争，传统金融机构也需要主动拥抱开源技术，以便更快地达成一流数字生态金融格局，把触角延伸到金融客户需求的方方面面。

从开发模式上来看，开源技术采用多人协作的开发模式，与传统闭源软件封闭式的开发模式相比，具有快速迭代、技术可扩展、技术路线寿命长等特点，在技术路径上相比于闭源软件更具有多样性和创新性。由于开源软件的代码是公开的，社区的参与者可以基于原有代码进行自由开放和修改，其技术更新迭代速度要比专有软件快得多，因此便于企业将更加优质的产品和服务快速推向市场。而售卖专有软件的公司往往更注重产品的成熟度和稳定性，在技术创新方面相对比较保守，因而导致专有软件的更新迭代速度和技术先进性可能落后于开源软件。金融机构在构建信息系统的过程中，可以借助开源的技术路径提升信息系统构建的先进性，助力金融机构科技创新。

另一方面，用于核心基础设施的专有软件会增加企业用户被供应商或技术锁定的风险，对于金融机构而言，选择专有软件可能会面临成本的提高和技术路线的限制，一旦供应商出现问题还可能影响到金融机构业务的连续性和稳定性。相比而言，开源软件的代码具有极强的透明性，不论是企业还是普通用户都能够获取开源软件的源代码。采用开源技术可以助力金融机构通过采用先进技术实现科技创新，进而推动业务健康快速发展。

三、 引入开源的风险日益凸显不容忽视

开源软件相比于闭源的商业软件，代码公开的好处显而易见，而背后开源许可证的复杂性却关注甚少，而引入开源的用户往往成为开源软件使用的风险落脚点，因此金融机构在引入开源的过程中应充分重视潜在风险问题。总体来看，金融机构作为开源用户可能涉及四类风险：运维和技术风险、管理风险、安全和数据风险、合规和知识产权风险。

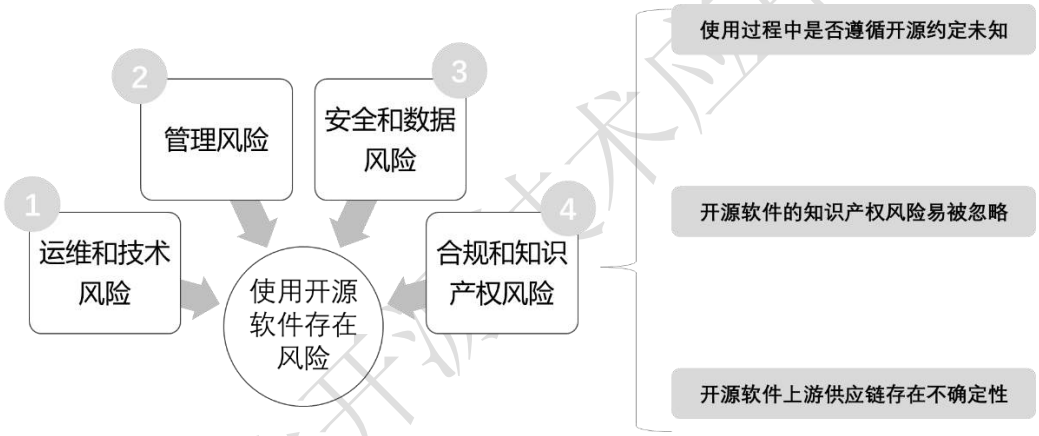


图 1 使用开源软件可能涉及的四类风险

1、 缺乏技术能力是企业用户的重要痛点

对于金融机构而言，开源软件与以往的闭源软件相比，最大的问题在于其需要本机构的开发运维人员自己负责管理和运维。在开发阶段，开源技术的开发难度要远大于直接购买配备厂商服务的闭源软件，因此往往要求企业配备更多相关人才，而人才的培养往往需要相对长的时间，也会消耗企业更多的资源。在运维

阶段，相对于闭源软件拥有完善的厂商服务，开源技术在很多情况下并没有相应的付费服务和运维支持，而金融机构本身的运维人员数量及能力都有一定限制，导致运维工作量大幅增加，开源技术相关运维问题解决困难。从整个生命周期管理角度来看，开源技术的社区版本更新速度远比闭源软件要快得多，其版本更新往往不存在第三方支持，金融机构被迫投入人力物力跟进开源技术发展，以避免因旧版本废弃或安全漏洞等问题导致的开源风险。

2、 是否引入开源软件难以完全准确统计

如果金融用户没有特殊要求，商业软件供应商一般不会说明其产品中是否涉及开源代码，甚至对用户号称完全自主研发，用户很可能被动引入开源软件。例如，2018 年国内某浏览器事件引起业内广泛关注，该浏览器一直对外宣称自主研发，然而经过行业测试却发现其使用了开源软件 Chrome 的内核。在此次事件之前，该浏览器在宣传或说明中未标注其使用了开源软件 Chrome。从开源合规的角度来看，该公司在自主研发中存在失信问题，同时也违背了开源许可证的署名要求。

从另一个角度来看，除了开源软件和组件，代码层级的开源使用问题也十分突出。在软件开发过程中，如果企业并未对源代码进行扫描，则很难从管理角度统一把控企业开发者是否在开发软件的过程中使用了开源代码片段。同时，对金融机构而言，存量软件及代码的规模相对更加庞大，对其进行代码合规

性检查的工作量更加巨大。因此，金融机构想要完全准确统计企业内引入开源软件的数目及真实情况在操作层面存在一定困难。

3、 开源软件隐含的安全风险较为显著

由于开源软件具有多人协作完成、开源许可证存在免责条款等特性，企业在使用开源软件时必须注意数据安全及隐私风险，若开源软件存有恶意代码、病毒或造成隐私泄露，将对金融机构带来较为严重的危害。总体来看，开源软件存在的安全问题较为严重，安全漏洞是主要的问题，后门等问题同样存在。开源软件的安全缺陷密度较高，据 SNYK 发布的《2019 年开源安全现状调查报告》显示，过去两年内应用程序的漏洞数量增长了 88%，仅 2018 年 NPM 的漏洞数量就增长了 47%。

以数据库领域为例，据安华金和最新发布《2019 年上半年数据库漏洞安全威胁报告》显示[1]，截止 2019 年 4 月，CVE 发布的被确认的国际主流数据库漏洞共计 81 个，其中 Oracle 9 个、MySQL 65 个。Oracle 被发现的 9 个漏洞中含 1 个超危漏洞，5 个高危漏洞；MySQL 数据库的 65 个漏洞中含有 2 个高危漏洞，62 个中危漏洞。由此可见，使用开源软件仍存在较大安全风险，金融机构在使用相应开源软件之前应进行充分评估，对安全漏洞予以重视。

[1] https://www.freebuf.com/company-information/158591.html

4、 使用过程中是否遵守开源约定未知

每一个开源软件都需要包含开源许可证去规定开源软件的使用范围和权利义务，金融用户在明确商业软件包含开源软件的前提下，很多情况并不能明确得知该软件是否遵守开源许可证的要求。开源许可证的基本要求包括：使用开源软件需要署名开源软件的作者或版权持有人的姓名或名称，需要明确使用哪一个开源许可证，并保留许可证全文或相关链接等等。

根据 GPL 许可证的规定，使用依 GPL 开源的软件并涉及到修改和分发时，用户需要将后续修改代码全部开源。例如，在 3D 打印领域，Marlin 是使用 GPL 许可证的开源软件，中国某企业引入 Marlin 后拒绝将修改部分依许可证规定对外开源，其结果是该公司被禁用开源软件 Marlin,在违反开源许可证规定的同时也可能面临法律制裁。

5、 开源软件上游供应链存在不确定性

对于金融用户而言，开源软件的上游供应链涉及开源基金会、开源产品及服务企业等。由于基金会开源软件的使用规则并不是一成不变的，开源软件存在修改开源许可证的可能性，从而导致开源软件许可使用方式的改变。例如，2018 年多个开源软件开发商已经对其过去使用的开源许可证进行了修改。2018 年 8 月，Redis Labs 由 AGPL 改成了 Apache v2.0 和 Commons Clause（共用条款）相结合的许可证；10 月，开源数据库 MongoDB 由 AGPLv3

改为一种新的服务器端公共许可证（SSPL），力求堵住基于云的服务带来的缺口；12 月，Kafka 修改 KSQL 许可证为 Confluent 社区许可证，禁止其作为 SaaS 产品来提供。目前的开源许可证变更与云服务相关的居多，但是金融机构作为开源软件的最终用户未来也可能会面临因开源许可证变化而导致的一系列风险，甚至可能影响已有开源软件的后续使用。

传统开源模式盈利模式开始遭遇瓶颈，各大开源公司/项目纷纷探索商业新模式。2018 年，Oracle 宣布 2019 年 1 月以后发布的 Oracle Java SE 8 公开更新将不向没有商用许可证的业务、商用或生产用途提供。对于以往使用 Oracle Java SE 8 的金融机构，如果希望能够继续获得支持就只能选择向甲骨文公司付费订阅，否则就只能选择开源的 OpenJDK 版本或者其他厂商的发行版。

同时，受开源基金会注册地法律规定影响，开源软件背后涉及的知识产权归属及开源软件未来是否受到限制使用等问题仍需引起足够重视。

6、开源软件的知识产权风险易被忽略

开源软件一般通过开源许可证约定其涉及的知识产权所属，然而一些开源许可证并未明确软件中涉及的知识产权问题。一部分开源许可证包含明确的专利许可条款，许可用户使用软件所包含的相关专利（需视许可证而有不同约定），如 Apache 2.0 和

GPL 3.0。另一部分开源许可证则没有明确说明，如 BSD、MIT 和 GPL 2.0。同时，为了防止有人恶意提起法律诉讼，部分开源许可证包含“专利报复”条款，如 Apache 2.0、GPL 3.0、AGPL 3.0 等。对于并未明确授予专利权的许可证而言，金融机构作为开源用户使用相关软件就可能存在潜在的风险。

开源的知识产权问题相对专业，一般的知识产权专家很难准确掌握开源许可证的责任义务要求，金融机构精通开源知识产权的专家相对匮乏，作为开源用户往往不能准确掌握常见开源许可证的使用方式，进而可能会埋下相应的风险隐患。

四、 金融行业开源治理建议

开源软件在金融机构中的使用日益广泛，同时其风险也日益凸显不容忽视。金融机构已经从理解开源的价值逐步走向认识开源的风险，后续也将从使用开源向治理开源方向转变。面对开源软件使用过程中的一系列问题，国家、金融企业和第三方机构应采取措施共同推动开源产业的健康有序发展，在充分保障金融机构满足合规要求的同时以开源新技术的应用促进金融机构向数字化、智能化方向转型。

1、 推广产业开源科普，树立开源风险意识

从国家层面来看，开源知识的科普和开源风险意识的树立至关重要。我国应培育开源发展的政策环境，完善开源相关法

律保护机制，加强开源软件的社会认知度和开源相关专业人才的培养，鼓励和推动开源社区发展，支持开源社区进行培训和研讨活动，整体上从国家或行业层面提高对开源的重视程度。

产业界可以通过开源白皮书和书籍的形式向相关企业和人员灌输正确的开源理念，针对开源的概念、开源许可证的要求进行解读，组织相关开源及知识产权专家进行演讲与培训，提醒企业引入开源可能面临的风险，树立金融机构作为开源用户的风险意识。

金融管理机构可以通过调查问卷的形式，对开源软件在金融业的应用情况进行调研，了解行业实际应用和管理状况，包括：一、开源软件使用基本情况，包括：使用原因、规模、核心业务系统应用占比等；二、开源软件引入和使用情况，包括：选型依据、测评方式、管理机制、更新频率等；三、开源软件应用评价，包括：影响和效果、风险和问题、对外部环境的诉求等。通过深入摸底金融行业对开源技术的使用和管理情况，分析现状及问题，后续形成调研报告供相关各方参考。

2、建立金融开源社区，增进同业交流沟通

金融机构作为开源软件的用户，相比于科技公司在开源领域的参与度较弱，且需求往往只能间接通过开源产品和服务提供商来反映问题提交建议。因此，在国内有必要建立具有金融行业属性的开源社区，通过集合多家金融机构，形成行业运作、交流、

共治平台，共同探索开源技术在金融行业更好的应用，以提升金融机构对开源的参与度。

国际方面已有针对金融领域的开源基金会，FINOS 于 2016 年建立，并运作良好，该基金会拥有 30 余家会员单位、70 余个项目正在孵化、300 余名社区贡献者，其核心董事会成员来自花旗集团、摩根大通集团等，社区非普通（白金、黄金、白银）会员均需要付费，普通会员需要对社区做出重要贡献方可免费加入。国内方面，目前中国信通院已经联合浦发银行等 10 余家金融机构及华为、腾讯等多家科技公司，共同成立了金融行业开源技术应用社区，探索非实体化的自发开源组织运作模式。运行资金主要来源于科技公司会员赞助；秘书处为轮流制，初期由中国信通院和浦发银行联合设置。经过半年多的运转，社区已经建立了章程规范，并形成了以“开源治理工作组”、“开源软件选型工作组”、“开源项目孵化组”为核心的运作模式，促进开源技术研究成果共享和开源产品在金融行业的应用。

3、 梳理开源治理规范，推动相关标准制定

针对国内开源产业相对缺少监管和规范的现状，第三方机构可以通过标准化的手段梳理用户侧使用开源应遵守的规范，中国信通院已经联合 30 余家金融机构和科技公司共同制定了《开源治理能力评价方法 第 2 部分面向开源用户》，通过标准的手段规范开源软件“申请-审批-使用”全流程管理，帮助金

融机构建立自上而下的开源治理体系。

通过相关标准的制定和评估的落地，促进金融机构规范开源软件管理，事先规避开源相关风险。进一步通过评估与行业内部交流，聚集最佳开源治理实践，推动业内形成共识，促进金融行业开源软件使用的规范化和全行业整体开源治理能力的提升。

4、 建设开源治理体系，规范开源软件引入

金融机构可以通过制定开源管理制度，建立企业内部开源软件管理平台，从公司层面对开源软件的引入和输出进行管理，构建全流程的开源治理体系，具体涉及组织架构、管理制度、软件选型、使用规范、风险管理、二次开发、持续跟踪、社区反馈和退出机制总共九个方面的内容。

1) 组织架构

从管理角度搭建开源治理相关的组织架构，设置明确的开源治理分工，将开源治理的工作和责任具体落实到个人。企业应在内部设立开源管理小组负责制定开源合规战略和开源治理流程，统筹规划和推动企业开源治理工作，并对开源软件使用全生命周期中涉及的各类角色的职责进行明确，具体包括管理、开发、运维、安全、法务等。

2) 管理制度

制定企业内部相关的规章制度，对开源软件的合规使用进

行管控，至少包括：开源软件引入制度、开源软件使用制度、开源软件漏洞检测制度、开源软件版本更新制度及开源软件退出制度等。

3） 软件选型

企业在引入开源软件时，可以从产品活力度、行业认可度、软件质量和服务支持能力四个方面进行选型评估，对软件进行综合评价并结合企业自身情况，进一步决定是否引入开源软件。具体可以参考代码托管平台上的项目数据、第三方评估报告，结合本企业的需求和内部评测流程，对开源软件是否能够引入进行综合评估。

4） 使用规范

开源技术在使用过程中存在风险，因此企业在使用开源技术时应依照规范根据引入需求确认测试范围，对开源软件的相关功能进行必要的测试。针对基础类软件应由负责部门编制软件使用说明文档，针对系统级别的开源软件应制定相应的应急预案，对于核心业务应保证至少有一个成熟的方案做备份。

5） 风险管理

企业在引入开源软件时应遵循统一的引入流程，并对建立开源软件统一管理机制，对企业所使用的开源软件信息进行记录（包括软件名称、作者、出处、版本号、许可证、正在使用的部门等）。针对开源许可证和安全两大方面的风险，应该定期进行评估并应设置专业人员（如法律人员、安全人员等）进行

风险处置指导，及时识别可能存在的风险点并建立与使用、运维、安全、法律等相关人员的沟通机制，确保在面临风险时能够及时妥善解决。

6） 二次开发

企业为满足业务场景需求可能会基于开源技术进行二次开发，此时首先对社区软件现有情况进行确认，包括社区现有功能、接口兼容性、接口版本、开源许可证要求等，设计出二次开发方案，进一步按照企业和社区规范进行编码、测试和发布。特别是对于涉及对外分发的应用场景（如手机 APP 等）的开源软件/组件，需要按照开源许可证的相关规定保留原版权信息并添加开发者的版权信息，如相关代码需要贡献给社区，在进行编码时应遵循开源社区的编码规范和要求。

7） 持续跟踪

在开源软件的使用过程中，企业应持续跟踪开源软件的各项情况，维护开源软件企业中的健康合规运行，包括社区情况、漏洞情况、版本情况、开源许可证情况等。对于长期不更新或社区活跃度极低的开源软件应予以重视；对于软件漏洞应由专门人员持续跟踪漏洞信息并及时反馈给软件使用方，并及时进行修复和处置；如出现开源许可证变动情况，应及时组织相关负责人结合本企业的风险接受能力评估相应开源许可证存在的风险。

8） 社区反馈

金融机构与科技公司相比，大多数情况作为开源软件的用户存在，但有时会涉及社区反馈的问题。当需要以企业名义进行社区反馈时，企业应对企业员工如何反馈开源社区进行规范，制定相关制度对员工申请开源的代码进行审查，并对社区贡献进行统计管理。重点需要评估该部分代码的开源是否会对业务造成影响（如涉及公司核心技术等），是否会因开源许可证的要求而导致公司其他代码面临被迫开源的风险，是否涉及专利商标等知识产权问题等。

9） 退出机制

作为软件生命周期管理的一部分，开源软件除了需要重视引入之外，还应重视起退出机制。企业应制定开源软件退出制度及退出规划，对停止使用的软件进行统一记录和管理。在面临产品替代、法律安全问题等情况时，应由开源管理小组统一对软件的退出流程进行规划，并按照规划进行迁移、替换、退出等操作。

除此之外，企业还可以通过建设内部开源治理支撑平台，保障开源治理工作的高效运行。通过平台化的手段实现金融机构内部开源软件的引入评估、使用评估、安全漏洞评估等工作的流程化和自动化，做到开源软件全生命周期的跟踪和记录。

附录 金融机构开源治理实践案例

中国农业银行

(一) 开源软件管理背景

随着云计算、大数据、人工智能、区块链等为代表的金融科技的发展，金融机构也纷纷通过引入开源软件来重塑银行信息系统的服务能力。尽管开源软件在金融机构获得了广泛认可，发挥着巨大的作用，但金融机构在引入、使用和管理开源软件的过程中，还存在着许多空白和不足。农业银行针对开源软件在金融行业的应用场景，构建了一套商业银行开源软件一体化管理体系，实现开源软件融合式管理，打造“五位一体”涵盖从引入到退出的全生命周期管理闭环；提出一套开源软件管理与使用规范，为开源软件管理建立执行标准；整合开源软件管理工具，打造覆盖全领域、全系统的开源软件管理平台，为开源软件管理提供落地保障。

(二) 开源软件管理体系

农业银行开源软件管理和应用是在监管部门相关政策的指引下，通过分析银行 IT 架构演进的特点，立足农业银行开源软件应用管理实践，提出了一套融合传统和开源理念的软件管理框架 TOSIM，以及使用于商业银行落地实施的开源软件管理规范标准和管理平台及工具。

1. TOSIM 开源软件一体化管理框架

农业银行在开源软件的管理过程中，针对开源软件和传统软件管理的特点，既兼顾开源软件和传统软件管理过程上的相似性，又关注到开源软件管理的特殊性与复杂性，提出了开源软件一体化管理框架 TOSIM，将开源软件管理融入到现有软件管理体系之中，按照系统化原则形成统一、协调、补充、兼容的有机整体。该体系包含两个维度，一是从管理体系维度打通开源软件管理涉及到的各项 IT 管理活动，形成架构管理、项目管理、安全管理、配置管理、运维管理"五位一体"的管理闭环，二是从模型、评估方法、制度流程、系统与工具、培训与实践的内容体系维度，实现开源软件融合式管理。

TOSIM 开源软件一体化管理框架有着如下的显著特点：

一是强调建立全面的管理体系。TOSIM 管理框架覆盖开源软件选型、评测、引入、使用、维护和退出全生命周期，从管理目标、业务流程到技术方法进行了全面阐述和指导，具有较强的可操作性、可落地性。

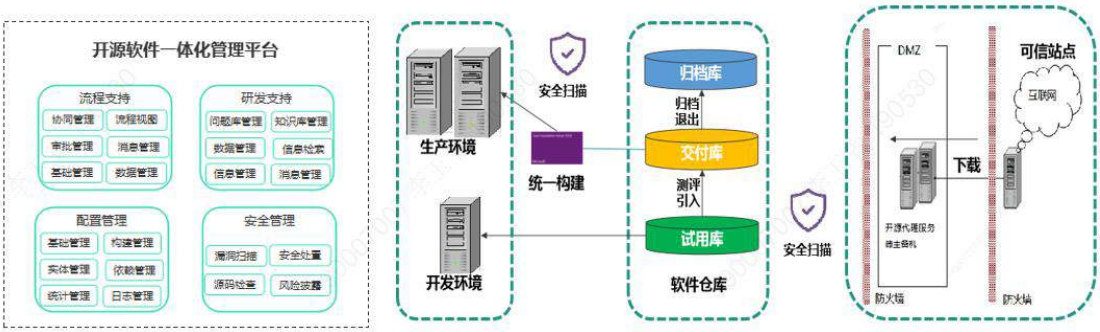
二是强调建立融合的管理体系。开源软件管理涉及面广、复杂度高，TOSIM 管理框架将开源软件管理融入现有的架构管理、项目管理、安全管理、配置管理等领域，给出了各领域开源软件管理的工作模型，强调跨部门、跨领域工作的高效有序衔接，为提高管理效率提供了有力保障。

三是强调建立分级分类的管理体系。TOSIM 管理框架践行"管理一体化，内容差异化"理念，充分考虑各类开源软件在不同

业务应用场景下的特点，针对不同种类开源软件的引入测评、配置管理、场景适用性、应急响应、漏洞处置等方面均提出差异化管理要求，避免“一刀切”等现象出现。

2. 管理平台与工具

开源软件一体化管理平台为 TOSIM 一体化管理框架的落地提供了重要的技术平台支撑。通过整合各方面技术资源，实现了开源软件全流程、多领域一体化管理，打通了开源软件从引入到退出的全生命周期管理流程，覆盖了架构管理、项目管理、安全管理、配置管理、运维管理等各个管理领域，支撑起开源软件管理的流程化、线上化、可视化，有效提升了开源软件管理质量和效率。



(三) 开源软件管理实效

目前，得益于农业银行开源软件管理体系，开源软件在农行 IT 系统中得到有效应用，引入了大量成熟开源产品和开源框架，构建了基于开源软件 Spring 体系为核心的企业级产品研发平台，通过提供完善的基础架构降低开发技术难度，让研发人员能够专注业务，快速开发出复杂的业务功能。建成了以 MPP 数据库和

Hadoop 深度融合的大数据平台，实现了 6.8PB 以上的结构化数据处理、4.8PB 的非结构化数据处理和毫秒级流计算处理。通过“采购+定制”方式建设了农行 PaaS 云平台，有力的推进了农行应用上云进程。

开源软件一体化管理体系在农行的实践表明了其科学性和可实施性，丰富和完善了农业银行架构生态，加速了应用领域赋能，降低了生产运行风险，推进了金融科技创新，为金融机构开源软件的管理提供了一个可参考的案例。

上海浦东发展银行

（一）概述

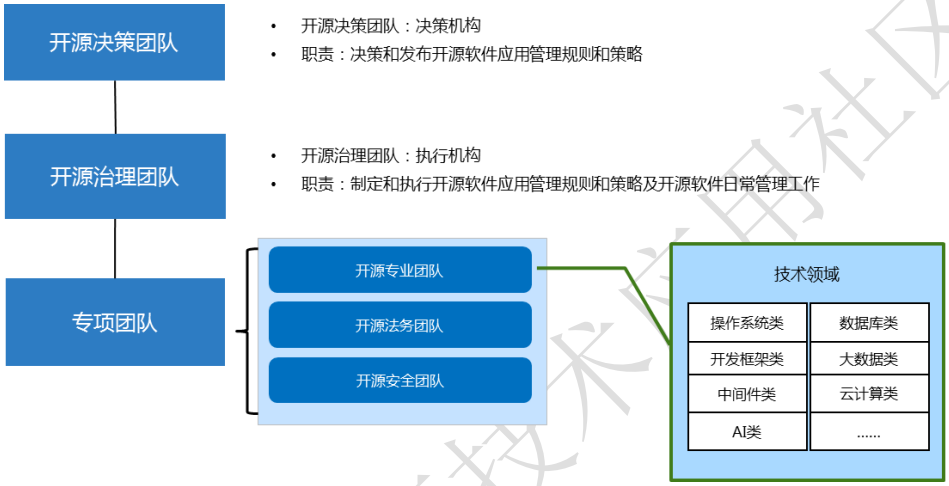
伴随着金融行业数字化转型的强烈需求，越来越多的银行应用系统会构建在开源软件之上，并享受其带来的订制灵活、功能丰富、迭代快速、人才资源集中等好处。但同时，开源软件有别于商用软件，其安全性、可靠性、可维护性以及许可遵从都会给银行科技建设带来新的挑战。银行需要在技术上、社区上、法务上全面评估和把控开源软件使用风险。浦发银行根据自身特点建设了开源技术治理体系，为未来自主、高效、安全地使用开源软件提供技术和制度上的保证。

（二）开源治理体系建设

开源治理体系是一套帮助浦发银行安全、合规、可靠、高效地评估和使用开源软件、管理开源软件资产、把控开源软件使用

中的安全风险的方法论和实践。治理体系贯穿于浦发银行现有的项目建设流程中，做到了开源软件全生命周期的管理覆盖，保障了浦发银行对开源软件的使用合理合规，在制度层面防范了开源软件的使用风险。主要包含以下五部分内容：

（1）开源治理的配套组织架构。



（2）开源治理的配套流程制度。指的是将开源治理要求嵌入到浦发银行现有信息系统项目建设中的一种流程制度。目前，我行已经在内部发布了《上海浦东发展银行开源软件应用管理规程》。其中包含了开源软件引入评估流程、开源软件使用流程、安全漏洞持续评估流程，以及即将新增的生命周期持续评估流程，源代码修改流程。

（3）开源软件评估评价方法。开源软件引入评估流程提供了科学的开源软件多维度评价视角，浦发银行依据 E- OSMM (Enterprise Open Source Maturity Model)模型以及华为开源治理的成功经验，结合银行行业特色以及浦发银行自身需求，形成了一套开源软件评估体系。

（4）开源软件治理支撑平台。一个用于支撑开源软件治理的平台系统，是整个开源治理工作高效运行的技术保障。目前平台已经实现流程平台、社区信息抓取、软件台账、漏洞跟踪、开源软件仓库等五大功能。截止目前，平台已经累计引入 451 个不同版本的开源软件，其中 151 个不同版本的开源软件通过引入并且介质维护入库。

通过自主研发的开源治理平台，把开源软件治理体系系统化，提高了管理效能，确保了开源软件应用台账的数据质量。管理平台中的软件仓库在技术上实现了开源软件实体介质来源可控可溯，直接服务于开发项目工程构件，提高开发效率。

（5）金融行业开源技术应用社区。一个非盈利性的组织，旨在通过信息共享，推动开源技术和软件在金融行业内安全可靠的使用。我行秉承了开源社区开放共享的精神，联合金融同业和 IT 服务商发起成立金融行业开源技术应用社区，主动分享治理成功经验，推动开源技术在行业内的进一步应用。。

（三）开源治理效能

1、有效防范了开源软件的使用风险

（1） 介质来源风险

浦发银行开源治理平台中包含的开源软件仓库是浦发内部唯一合法的开源软件介质来源。介质由开源治理团队从开源软件官网或认证的其他代码托管网站获取，保证其来源安全可溯，无植入后门或木马。

（2） 技术应用风险

开源治理体系科学评估了引入开源软件的版本和生命周期，保证引入软件尽可能得到社区的长期支持。并且开源治理体系还对开源软件的使用做了技术收敛，使得银行将有限的技术力量投入到受限的开源技术领域中，确保充足的技术储备和支持能力。

（3） 安全漏洞风险

开源治理体系提供了全周期的安全漏洞管理。实现了特定开源软件安全漏洞披露后在浦发银行业务系统中整改情况的跟踪，最大程度上规避安全漏洞风险。

（4） 法务合规风险

开源治理体系在引入开源软件过程中获取开源软件的许可证信息。通过开源软件应用台账，能方便的匹配到相应的业务系统。对于存在软件分发情况的业务系统，能及时要求相关项目组履行开源义务，做到合法合规。

2、主动拥抱开源生态，加速数字化转型

相比商业闭源软件，开源软件源码公开的特点使得二次开发更加容易，避免了商业软件无法及时应对特定需求的情况，摆脱了商业软件功能上的束缚，软件开发可以将焦点更多转向业务创新，使得浦发银行获得更多具有竞争力的定制化产品和独特功能。相比受限于商业软件无法订制特点的竞争对手，在数字化转型的战略中获得先机。在这个过程中，完备的开源治理体系是浦发银行大胆引入和应用开源软件的坚实基础。

3、大力促进行业交流，形成合力

作为开源治理体系建设的一部分，浦发银行发起成立了金融行业开源技术应用社区，集合了金融行业对在开源软件使用中共同的需求特点，以及各家单位对开源技术的使用经验，开展各种形式的同业沟通和交流，分享开源软件技术使用中的经验，共同应对开源软件金融行业的使用风险，促进开源技术在行业范围内规模化的应用。

中信银行开源

中信银行在开源治理方面进行了有益的尝试。总体上对开源软件秉持审慎引入、逐步推广、分级掌控原则。

（一）开源软件的引入

引入开源软件需要经过业内调研、验证测试、架构决策等环节。通过对有影响力的同业金融机构及互联网企业对待引入的开源软件的调研，深入了解软件的适用场景、运维及安全等相关方面的问题，初步评估是否有必要引入该软件；正式引入该软件之前，使用实际业务对该软件进行测试验证，依据调研报告及测试报告做架构决策。同时，引入的开源软件还必须符合中信银行整体架构转型的要求。如果同一类型的软件有多款，比如开源数据库有 MySQL、MariaDB、PostgreSQL 等。在具体选型时主要遵循软件成熟、可靠优先、兼顾性能、社区活跃的原则。软件成熟度主要依据装机量和业务口碑及公开缺陷数来评判；在可靠性维

度上，通过设计操作系统、CPU、内存、磁盘、文件系统、网络、软件等故障，在真实的业务场景中通过正常场景、异常场景、性能场景下验证其可靠性；社区活跃维度，则主要依据这款软件开源参与人数、缺陷修复速度、业内从业人数、网络搜索热度等评判；同时作为金融企业，该软件许可协证及是否能得到可靠的商业服务支持，也是评价该软件的重要依据之一。

（二）开源软件的推广

开源软件引入后，一般要经历非重要业务系统的小范围试点，再逐步向重要业务系统推广的过程。并通过一系列规范沉淀过程中使用经验和最佳实践，提高开发、测试、运维的水平。规范一般包括开发规范、设计规范、迁移指引、接入规范、部署规范、运维规范等。同时，中信银行的实践表明，培训是开源软件推广的重要环节。通过密集的外部和内部培训，能快速提升该开源软件的应用水平。另一个有益的实践是开源软件专家深入应用的设计、开发、测试等环节，提升基于该软件的开发质量，减小推广阻力。

（三）开源软件的掌控

中信银行对开源软件的重要性定级，依据该软件所支撑的业务系统的重要性等级，按照就高不就低的原则确定。掌控分为 4 级：一级掌控要求掌握其设计和实现；二级掌握要求掌握其核心模块的设计和实现；三级掌控要求掌握其核心模块的设计；四级掌控要求熟练使用该软件。对于 A 类以上系统，要求一级掌控。

对于一级掌控要求的开源软件，中信银行鼓励参与开源社区的建设，跟踪其发展方向。中信银行尽量减少对开源软件的定制，避免形成分支版本后面临的升级压力。如业务必须定制，要求将定制的代码提交开源社区。

在版本的控制方面，中信银行的策略是尽量使用成熟稳定的版本。基础软件的升级是一项非常消耗资源的工作，是否必须升级由多种因素决定。而选择开源软件的一个好处是“不再被软件厂商强制升级”，中信银行有决定是否升级的能力。我们对软件性质进行分类：对于计算类软件，升级代价和风险可控，可以因为一些需要引入的新特性而进行升级；对于数据存储类软件，升级代价和风险相对高很多，我们会谨慎评估。但不管哪一类软件，只要涉及到“安全相关”的缺陷，都要进行及时的升级。

中国太平洋保险（集团）

（一）背景

随着集团信息中心数字化转型与互联网、大数据应用的迅速发展，大量开源软件涌入太保，我们在受益于开源技术的同时，也意识到开源技术管理的困难与风险。我们需要一些方法和流程来规范开源技术的管理，努力从“被动接受“向有计划、有目标的“主动探索“转型。

（二）阶段性成果

通过集团内部问卷、现场调研，梳理现有开源技术的使用情

况，通过同行业、互联网开源技术领域的专家的技术经验交流。从 2018 年初至今，设定了开源技术导入标准流程、开源技术导入评估模型的落地以及开源实验室的初步创立，形成了从管理、流程、制度、方法等维度的开源技术统一的管理框架。

1、开源技术导入标准流程

通过不断的摸索和实践的打磨后，确定了如下的开源技术导入标准的流程：

在流程的不同阶段，形成各个阶段不同的交付物。生产、开发、设计等部门提交《开源技术导入申请表》后，根据模型评估的五大纬度进行逐项评分并提供评分依据后落地《开源技术评估结果》，然后组建 POC 团队并明确 POC 的目标和要求，落地 POC 的测试报告。经由专家会诊后，形成《专家委员会评审报告》后导入开源技术库，用户可以自行下载该项技术落地的《开源技术基本信息》、《安装配置手册》、《运维手册》、《用户手册》等相关文档。

2、开源技术评估模型

结合问卷、现场等形式的调研，以及集团对开源技术的使用情况、开源技术知识储备以及安全生产等多个维度的综合考量，

形成产品生命力、技术适用性、安全保障、本地化服务、商务友好性等 5 个维度的评估模型。产品生命力是从技术框架所在社区和技术框架本身评估是否有比较强的生命力；技术适用性是评估技术框架是否符合企业 IT 现有特征，适合在企业内使用；安全保障是评估技术框架是否满足企业对安全的要求；本地化服务是评估产品是否具备比较好的本地服务能力；商务友好性是评估产品是否在商务上有授权限制，授权和维护费用是否有竞争力。

3、开源实验室

开源实验室分是由实验室经理领导管理，各个技术领域的专家组成。目标是共同管理维护太保的开源技术生态圈。现阶段主要负责开源技术相关的分析、模型评估、POC 验证、技术引入等职责，从组织架构的维度对开源技术进行管理、维护和深入研究。

（三）开源技术实用化尝试

1、模型的实用化使用

在开源实验室经理的领导下，组织开源实验室技术专家和开源技术委员会结合开源技术的特性，对评估内容进行调整并确认评审内容是否完整，不断修正模型评估维度细项，并不断收集基础信息调整模型的输入，以保证模型评估结果的准确，保障开源技术引入后的生产的稳定运行。

2、开源技术库的实用化使用

开源技术库是由版本库、指标库、知识库、开源技术社区组成的。版本库是记录所有满足太保导入标准的开源软件的详细信

息,及该产品有效使用时间；指标库是通过定期审计,记录开源软件使用情况进行追踪及记录；知识库是记录开源软件的安装配置手册,运维手册等,给各个部门需要使用该开源技术的同仁提供帮忙；开源技术社区是提供一个员工对技术畅所欲言的地方,对开源技术库中的产品使用过程中遇到的任何问题或建议进行讨论。